Appeal No. 2024-2256

IN THE UNITED STATES COURT OF APPEALS
FOR THE FEDERAL CIRCUIT

LARRY GOLDEN,

Plaintiff-Appellant,

v.

UNITED STATES,

Defendant-Appellee.

On Appeal from the United States Court of Federal Claims in
Case No. 1:23-cv-00811, Senior Judge Eric G. Bruggink

EXHIBITS IN SUPPORT OF DEFENDANT-APPELLEE
UNITED STATES' MOTION FOR SUMMARY AFFIRMANCE

BRIAN M. BOYNTON
Principal Deputy Assistant Attorney General

SCOTT BOLDEN
Director

Of Counsel:
CONRAD J. DeWITTE, JR.
Department of Justice

GRANT D. JOHNSON
Trial Attorney
Commercial Litigation Branch
Civil Division
Department of Justice
Washington, DC 20530
T: (202) 305-2513

Appeal No. 2024-2256

TABLE OF CONTENTS

<p style="text-align:center; color:red;">**CORRECTED**</p>

In the United States Court of Federal Claims

No. 23-811C
(Filed: April 23, 2024)

* *

LARRY GOLDEN,

        Plaintiff,

v.

THE UNITED STATES,

        Defendant.

* *

    Larry Golden, pro se.

    Grant Johnson, Trial Attorney, United States Department of Justice, Civil Division, Commercial Litigation Branch, Washington, DC, with whom were *Brian M. Boynton*, Principal Deputy Assistant Attorney General, and *Scott Bolden*, Director, for defendant.

<p style="text-align:center;"><u>ORDER</u></p>

BRUGGINK, *Judge*

    Plaintiff Larry Golden, appearing *pro se*, filed his most recent, fourth complaint in this court on May 31, 2023. In it, Mr. Golden alleges the United States, through the Defense Threat Reduction Agency "authorized or consented" to the use of Google phones that infringed on the same patents[1] as those previously asserted in his first case, filed in 2013 ("*Golden I*"). Compl. ¶ 21 (the present case is "*Golden IV*"). Except for the manufacturer of the accused devices and the agency alleged to have authorized the

---

[1] Those are U.S. Patents No. 10,163,287, 9,589,439, and 9,096,189. A fourth patent, not asserted in this case, was also alleged to have been infringed in *Golden I*.

<p style="text-align:center;">**A001**</p>

infringing use, the present case is otherwise virtually identical to plaintiff's first patent complaint.

In *Golden I* (Case No. 13-307), plaintiff alleged that the government infringed the claims of five related patents through a Department of Homeland Security ("DHS") initiative known as "CELL-ALL." Eventually, he identified virtually all cell phones manufactured by Apple and Samsung after the 2011 DHS initiative as infringing. After plaintiff amended his complaint six times, *Golden I* was dismissed on November 10, 2021, with prejudice for failure to conform his infringement contentions to the court's rules. *Golden v. United States*, 156 Fed. Cl. 623, 632 (2021). Plaintiff appealed, and the Federal Circuit affirmed the dismissal on September 8, 2022. *Golden v. United States*, No. 2022-1196, 2022 WL 4103287 (Fed. Cir. 2022). Mr. Golden also filed two other actions in this court, founded on constitutional theories, which are not germane to the present issues.[2]

Mr. Golden also recently brought his theories to the federal district courts in South Carolina and California, asserting similar patent claims to those here against Google and other companies. We need not discuss all of the litigation that those complaints have spawned. What is relevant here, however, is that Mr. Golden filed infringement claims against Apple, and others, in the District of South Carolina which were dismissed as frivolous. On appeal, however, the Federal Circuit reversed, holding that the Apple

---

[2] Plaintiff filed his second action on January 17, 2019, alleging a Fifth Amendment taking based on the Patent Trial & Appeal Board's cancellation of certain claims of another of plaintiff's patents during an *inter partes* review ("IPR") ("*Golden II*"). The court dismissed *Golden II* with prejudice on May 14, 2019, finding that the cancellation of the patent claims was plainly the result of plaintiff's voluntary amendment, not government action. *Golden v. United States*, No. 19-104C, 2019 WL 2056662 (Fed. Cl. 2019) ("*Golden II*"). The Federal Circuit also affirmed this dismissal. *Golden v. United States*, 955 F.3d 981 (Fed. Cir. 2020).

Plaintiff filed his third action here on February 7, 2023, again on the grounds that DHS took one of his patents during the IPR without compensating him. *See Golden v. United States*, No. 23-185C, 2023 WL 4466401 (Fed. Cl. May 30, 2023) ("*Golden III*"). Before granting the government's motion to dismiss for lack of jurisdiction on statute of limitations grounds, we noted that *res judicata* would otherwise clearly bar the claim due to its near-identical nature to the claims proposed in *Golden II*. *Id.*, *aff'd*, No. 2023-2139, 2023 WL 8663093 (Fed. Cir. Dec. 15, 2023).

2

A002

complaint was not facially frivolous, but the court took no position on the merits of the infringement claim itself. *Golden v. Apple, Inc.*, No. 2022-1229, 2022 WL 4103285 (Fed. Cir. Sept. 8, 2022). As discussed later, a misunderstanding of the import of that decision was the impetus for plaintiff's instant case.

In the present suit, defendant has moved to dismiss on the basis that Mr. Golden's claim is barred due to the preclusive effect of the judgment entered in *Golden I*.[3] Plaintiff has since filed a motion for summary judgment, arguing that the Federal Circuit's reversal of the South Carolina district's dismissal is grounds for judgment in his favor here. Mr. Golden notes in that motion that the elements of the accused devices in this case and those in the South Caroline case are "virtually identical." Mr. Golden also filed a motion for disqualification of the undersigned on the grounds of coercion and "difficulty," or, in the alternative, bias. Lastly, plaintiff filed two motions for judicial notice, the first regarding certain facts he believes relevant to his theory of infringement, and the second concerning filings he made in one of his cases in the Northern District of California.[4] Because, as explained below, the complaint fails to state a claim upon which relief can be granted, we need not reach any of the latter motions. The motion for disqualification we deny.

Defendant argues that plaintiff's claims against the government accusing Google phones are barred by the doctrine of claim preclusion, traditionally known as *res judicata*, because the newly accused devices are virtually identical to the devices he has previously accused. The government argues that, because his prior case was dismissed with prejudice, which operates as a judgment of non-infringement, his new claim is also barred because it has already been decided. *See Hallco Mfg. Co. v. Foster*, 256 F.3d 1290, 1297 (Fed. Cir. 2001) ("a dismissal with prejudice . . . is a judgment on the merits"). Put another way, because there is no practical difference, at least as to the features alleged to be infringing, between the Google phones now accused and the Apple and Samsung products previously accused, there is nothing new to be decided now. The thing has been decided

---

[3] Defendant also argues that plaintiff's theory of infringement is facially defective and fails to state a claim. We do not reach this issue because the complaint is plainly barred by *res judicata* and the associated *Kessler* doctrine.

[4] Plaintiff also filed a motion to strike defendant's motion to dismiss, which we denied by order on July 31, 2023.

3

A003

("*res judicata*"). Further, to the extent that our judgment in *Golden I* would not cover any alleged infringement post-dating that judgment, defendant argues that the *Kessler* doctrine expands the reach of claim preclusion to cover those allegations as well. *Kessler v. Eldred*, 206 U.S. 285 (1907) (206 U.S. 285 (1907) (Holding that a judgment of a product's non-infringement may not be re-litigated, even if the parties are different and the alleged infringement post-dates the earlier judgment).

The doctrine of *res judicata* prevents re-litigation of claims previously decided. *See generally Sharp Kabushiki Kaisha v. ThinkSharp, Inc.*, 448 F.3d 1368, 1372 (Fed. Cir. 2006)**.** The current complaint, however, is aimed at different infringing devices, Google phones, not expressly implicated in *Golden I*. Defendant, however, argues that, because there is no substantive difference between the phones now implicated by the present complaint and those alleged to be infringing in the earlier case, claim preclusion applies. We agree.

In the Federal Circuit, claim preclusion in a patent suit generally applies "when a patentee seeks to assert the same patent against the same party and the same subject matter." *Senju Pharm. Co. v. Apotex Inc.*, 746 F.3d 1344, 1349 (Fed. Cir. 2014). The same patents and the same parties are clearly involved. The question then is whether the Google phones are the same as the subject of the previous suit. They are, of course, not literally the same phones. As defendant rightly points out, however, the subject matter is the same for claim preclusion in an infringement suit if the formerly accused and the newly accused devices are "essentially the same." *Foster v. Hallco Mfg. Co., Inc.*, 947 F.2d 469, 479-80 (Fed. Cir. 1992). They are essentially the same if the new devices are "materially identical . . . [to the earlier devices] with respect to the pertinent claim limitations at issue." *Nystrom v. Trex co., Inc.*, 580 F.3d 1281, 1286 (Fed. Cir. 2009). The focus is thus on what is claimed to be infringing in the new devices to see whether it is "essentially the same" as what was claimed to have been infringing in the old devices. Here, as explained below, the elements in these new phones that Mr. Golden alleges to be infringing are the same as those he claimed to be infringing in *Golden I*. Thus, claim preclusion applies, at least as to pre-*Golden I* judgment infringement.[5]

---

[5] Any alleged infringing acts after the judgment in *Golden I* are not barred by claim preclusion because they do not arise from the same transactional facts, or "infringing acts." Definitionally, post-judgment infringement cannot be the same acts already considered, and thus the claims cannot be the same for purposes of claim preclusion. *See, e.g, Brain Life, LLC v. Elektra Inc.*, 746 F.3d 1045, 1054 (Fed. Cir. 2014). Absent the *Kessler*

4

A004

In the present complaint, Mr. Golden concedes that his current claim is "virtually identical" in that "the results are the same" when compared to devices also accused in *Golden I*. Compl. ¶ 17; *see also* ¶¶ 18-20. Further illustrating that the subject matter is essentially the same in this suit as his first, the complaint also contains a comparison between the Google Pixel 5 phone and the Apple iPhone 12, Samsung Galaxy S21, and LG V60 phones. The latter three of those phones were all accused by plaintiff in *Golden I*, as evidenced by the Corrected Claim Chart filed by Mr. Golden there, excerpts of which were appended to defendant's motion to dismiss in this docket, which we treat as judicial admissions by Mr. Golden. Plaintiff went on to explain on page 13 of the present complaint that the use of the Pixel 5 phone is illustrative of the infringement of the other Google phones that he is accusing in this suit. Thus we are assured that all of the newly alleged infringement overlaps with what he claimed in *Golden I*. Even a cursory review of the rest of the present complaint—the comparison of devices mentioned above—reveals that they are materially identical to the charts filed in *Golden I*. The same elements of the Apple, Samsung, and LG phones alleged to be infringing in the first suit are what he accuses now in the Google phones, as illustrated by the Pixel 5 claim chart in his complaint (e.g., a central processing unit, GPS, wifi or Bluetooth connectivity, and biometrics). In fact, he performs the comparison himself in the present complaint again by including a comparison of the Apple, Samsung and LG devices with the Google Pixel 5. The subject of the two suits is "essentially the same" because the devices are identical with respect to the elements plaintiff claims are infringing.

The Federal Circuit has on several instances stated that claim preclusion has a temporal limitation as to the date of the preclusive judgment. *E.g.*, *In re PersonalWeb Techs. LLC*, 961 F.3d 1365, 1376 (Fed. Cir. 2020). The government thus invokes the *Kessler* doctrine as covering the "temporal limitation" gap of claim preclusion. In *Kessler v. Eldred*, the Supreme Court adopted an enlargement of traditional claim and issue preclusion doctrines to further preserve the utility of previous judgments of non-infringement by holding that a prior judgment of non-infringement would bar new

_____

doctrine, the issue of whether a prior judgment of non-infringement was preclusive of post-judgment acts would be considered under the rubric of issue preclusion, also known as collateral estoppel. Collateral estoppel was not raised by the government, nor need it have been, because, in the patent context, as will be discussed below, *Kessler* enlarges the reach of non-infringement judgments, or, as defendant puts it, bridges the temporal gap left by claim preclusion.

5

A005

infringement claims for post-judgment acts, against third parties, and covering very similar accused devices. 206 U.S. 285 (1907); *see also SpeedTrack, Inc. v. Office Depot, Inc.,* 971 F.3d 1317, 1318 (Fed. Cir. 2015) (recognizing that, absent *Kessler*, patent holders could escape prior judgments of non-infringement by suing customers of the earlier defendant for post-judgment infringement). The key issue is whether the accused devices are the same or "essentially the same," just as with claim preclusion. *Brain Life, LLC v. Elektra Inc.*, 746 F.3d 1045, 1057 (Fed. Cir. 2014). If so, pursuant to *Kessler*, a trade right in the devices attaches after a judgment of non-infringement and those devices, along with others that are "essentially the same," are protected from future allegations of infringement. *In re PersonalWeb*, 961 F.3d at 1379. As explained above, the newly accused devices are essentially the same as those previously accused, and thus doctrines of *res judicata* and *Kessler* preclude litigating these issues against the government again.

Plaintiff's only argument is that, because the Federal Circuit reversed and remanded the decision of the District Court for South Carolina in *Golden v. Apple Inc.*, we should overlook *Kessler*. In Mr. Golden's view of the circuit's opinion, infringement has been established. That, however, is a dramatic misreading of the appellate opinion. The Federal Circuit was careful to note that it "express[ed] no opinion as to the adequacy of the complaint or claim chart except that it is not facially frivolous." *Golden v. Apple Inc.*, No. 2022-1229, 2022 WL 4103285, at *2 (Fed. Cir. Sept. 8, 2022). Nothing in the Federal Circuit's opinion is germane to the questions of claim preclusion and the *Kessler* doctrine, both of which we find preclude consideration of the present complaint because the devices accused are, as conceded by plaintiff, "virtually identical," or "essentially the same" as those already adjudged in the first suit, *Golden I.* Compl. ¶17.

The Federal Circuit was recently confronted with a similar situation in which the patentee had infringement claims dismissed with prejudice for discovery abuses. When that patentee brought a later suit, accusing different devices, the district court dismissed it, *inter alia*, as precluded by *Kessler*. The Federal Circuit affirmed, holding that a dismissal with prejudice, whatever the underlying reason, is a judgment of non-infringement for purposes of the *Kessler* doctrine. *Askan v. FARO Techs., Inc.*, 2023 WL 4101351, at *3 (Fed. Cir. June 21, 2023). Thus, because the devices were found to be essentially the same, *Kessler* applied. *Id.* at *4. Here, Mr. Golden's claims in his first suit were dismissed with prejudice. 156 Fed. Cl. at 632. As explained above, the newly accused devices are essentially the same as those previously alleged to be infringing, as plaintiff admits. Thus,

6

A006

Kessler applies, and the present claim is barred. Accordingly, the following is ordered:

1. Plaintiff's motion seeking disqualification of the undersigned is denied.

2. Defendant's motion to dismiss is granted.

3. The Clerk of Court is directed to dismiss the complaint pursuant to rule 12(b)(6) for failure to state a claim.

4. All other motions are denied as moot.

<div align="right">
s/ Eric G. Bruggink
ERIC G. BRUGGINK
Senior Judge
</div>

7

A007

In the United States Court of Federal Claims

No. 23-811 C
Filed: April 24, 2024

```
**********************************
LARRY GOLDEN,                    *
           Plaintiff,            *
                                 *          JUDGMENT
      v.                         *
                                 *
                                 *
THE UNITED STATES,               *
           Defendant.            *
**********************************
```

     Pursuant to the court's Order, filed April 23, 2024, granting defendant's motion to dismiss,

     IT IS ORDERED AND ADJUDGED this date, pursuant to Rule 58, that plaintiff's complaint is dismissed for failure to state a claim.

                           Lisa L. Reyes
                           Clerk of Court

                     By: *Ashley Reams*
                          Deputy Clerk

NOTE: As to appeal to the United States Court of Appeals for the Federal Circuit, 60 days from this date, see RCFC 58.1, re number of copies and listing of all plaintiffs. Effective December 1, 2023, the appeals fee is $605.00.

A008

In the United States Court of Federal Claims

No. 23-811C

(Filed: July 30, 2024)

* * * * * * * * * * * * * * * *

LARRY GOLDEN,

        Plaintiff,

v.

THE UNITED STATES,

        Defendant.

* * * * * * * * * * * * * * * *

ORDER ON RECONSIDERATION

Plaintiff Larry Golden, appearing *pro se*, filed his fourth complaint in this court on May 31, 2023, alleging that the United States government, acting through the Defense Threat Reduction Agency ("DTRA"), implicitly authorized the use of three of his patents by several third party corporations in violation of 28 U.S.C. § 1498(a). On April 23, 2024, the court dismissed plaintiff's claim pursuant to Rule 12(b)(6) of the Rules of the United States Court of Federal Claims ("RCFC"), finding that his claim was barred by claim preclusion and the related *Kessler* doctrine. *Golden v. United States*, 171 Fed. Cl. 33, 37 (2024) (relying on *Kessler v. Eldred*, 206 U.S. 285 (1907)). Plaintiff filed a motion for reconsideration and notice of pending motion for disqualification on April 30, 2024, asserting that the court's dismissal of his claim had been rooted in racial bias and was not in accordance with the doctrine of vertical *stare decisis*.

Turning to the present motion, although denominated as a motion for reconsideration, it appears that the thrust of the motion is aimed at disqualification of the undersigned, but we note that most of the arguments in support of that relief are disagreements with the merits of our dismissal decision.[1] We begin by noting that there is no provision in the court's rules

---

[1] We are unsure if plaintiff's notice of pending motion for disqualification is a reference to his earlier-filed motion, which was disposed of in our opinion

1

A009

for the filing of a post-judgment motion for disqualification. Plaintiff cites 28 U.S.C. § 144 as grounds for the requested disqualification. That statute, by its very terms, however, applies only to the federal district courts, and not to the Court of Federal Claims. 28 U.S.C. § 144 ("Whenever a party . . . *in a district court* makes and files a timely and sufficient affidavit that the judge before whom the matter is pending has a personal bias or prejudice . . . such judge shall proceed no further therein.") (emphasis added). Nor would such a request be timely after judgment has been entered. We thus consider the motion under the rubric of reconsideration.

Motions for reconsideration are governed by Rule 59(a)(1) of the Rules of the United States Court of Federal Claims ("RCFC"). Pursuant to Rule 59(a)(1)(A), "the court may, on motion, grant . . . a motion for reconsideration on all or some of the issues . . . for any reason for which a new trial has heretofore been granted in an action at law in federal court." A motion for reconsideration may also be granted "for any reason for which a rehearing has heretofore been granted in a suit in equity in federal court; or upon the showing of evidence . . . that any fraud, wrong, or injustice has been done to the United States." RCFC 59(a)(1)(B–C). Specifically, RCFC 59 permits reconsideration for one of three reasons: 1) an intervening change in the controlling law has occurred; 2) previously unavailable evidence is now available; or 3) the motion is necessary to prevent manifest injustice. *Matthews v. United States*, 73 Fed. Cl. 524, 525 (2006). Furthermore, "the movant must point to a manifest error of law or mistake of fact" and must do more than "merely reassert[] arguments which were previously made and were carefully considered by the court." *Henderson Cnty. Drainage Dist. No. 3 v. United States*, 55 Fed. Cl. 334, 337 (2003). A motion under RCFC 59 "must be based upon manifest error of law, or mistake of fact, and is not intended to give an unhappy litigant an additional chance to sway the court." *Parsons ex rel. Linmar Prop. Mgmt. Tr. v. United States*, 174 Fed. Appx. 561, 563 (Fed. Cir. 2006).

Plaintiff does not argue a change in the controlling law or offer any newly discovered evidence. Instead his motion largely restates arguments he made in his complaint. Mr. Golden presents four broad reasons for why he believes our previous opinion should be reconsidered. First, he alleges that our opinion runs afoul of the doctrine of *stare decisis*. Second, he argues that his Fifth Amendment due process rights have been violated. Third, plaintiff argues that we misapplied the doctrine of res judicata, or claim preclusion. Fourth, plaintiff suggests throughout his motion that our opinion was

---

of April 23, or whether plaintiff intends to convey that he is asking for that same relief in this motion.

motivated by racial bias, though he does not point to any specific evidence or details that support this allegation. We address these four arguments in turn.

Plaintiff argues that the doctrine of *stare decisis* requires the Court of Federal Claims to follow the decisions of the Court of Appeals for the Federal Circuit, specifically the circuit court's decision in Mr. Golden's appeal from the dismissal of his claims in district court in South Carolina. We note, to start, that that decision is not the law of this case because it was not an appeal in this case. It is also unpublished and thus, by the circuit's own rules, not binding precedent. *See* Fed. Cir. R. 32.1(d). It is persuasive authority only to the extent that it prescribes some rule of law applicable to the issues in this case. It did not. The issue there was whether plaintiff's pleadings were facially frivolous. *Golden v. Apple Inc.*, No. 2022-1229, 2022 WL 4103285 (Fed. Cir. Sept. 8, 2022). The issue here was whether the doctrine of claim preclusion, as expanded by *Kessler*, barred relitigation of the issue of infringement. *Golden*, 171 Fed. Cl. at 37.

As we observed in our dismissal opinion, plaintiff has fundamentally misunderstood the Federal Circuit's ruling in *Golden v. Apple Inc*. The present motion raises no new argument in this regard, and the argument he does make hinges on a "dramatic misreading of the appellate opinion." *Id.*

Next, plaintiff alleges that his Fifth Amendment due process rights have been violated, because the court has allegedly deprived plaintiff of his property through "unfair and unjustified" means. Mot. Recons. 2. Though not clear, his argument seems to be that he should have won his case on its merits, and because he did not, his due process rights have been violated. Plaintiff has not identified any process that was due him and which was denied. His claims were barred by *res judicata*. That is not a violation of due process. *See Searcy v. Dep't of Agriculture*, 813 Fed. App'x 472, (Fed. Cir. 2011) (holding that the Merit Systems Protection Board did not violate the appellant's due process rights by *sua sponte* dismissing the claim as barred by *res judicata*). As the Supreme Court has explained, the fundamental requirements of procedural due process are notice and opportunity to respond, both of which are met here. *Cleveland Bd. Of Educ. v. Loudermill*, 470 U.S. 532, 546 (1985).

As to *res judicata* itself, plaintiff argues that "issue preclusion"[2] does not apply here and is inapplicable to his infringement claims. He calls the

---

[2] We understand plaintiff to actually be referring to claim preclusion, which was the grounds for his complaint's dismissal.

Kessler doctrine a "special" preclusion doctrine "created" by the Federal Circuit which should not apply here, because it supersedes congress' intent to allow patent infringement suits to be brought against the government "whenever" under 28 U.S.C. § 1498(a). Mot. Recons. 4. Plaintiff is wrong. The doctrine of *res judicata* applies to all claims at law and equity. It protects the preclusive effect of judgments and preserves the court's and prevailing parties' resources by preventing relitigation of previously decided claims. *See Montana v. United States*, 440 U.S. 147, 153–154 (1979) (stating that *res judicata* protects against the "expense and vexation attending multiple lawsuits, conserves judicial resources," and minimizes the "possibility of inconsistent decisions."). We have applied *Kessler* before in the section 1498 context. *See, e.g.*, *JG Techs., LLC v. United States¸* 156 Fed. Cl. 691, 713 (2021) (finding that certain of plaintiff's infringement claims against the United States were barred by *Kessler*).

In Mr. Golden's view, we have unduly relied on the previous cases in which Golden lost. As explained in April, however, the doctrine, as expanded by *Kessler*, applies, and it bars plaintiff's latest complaint. *Golden*, 171 Fed. Cl. at 37. This motion for reconsideration casts no doubt on that result.

Lastly, we address the allegations of racial bias which plaintiff peppers throughout his motion without substantiation or citation to evidence outside of his disagreement as to the disposition of his cases. An adverse result is not evidence, by itself, of bias. *See Liteky v. United States*, 510 U.S. 540, 555 (1994) ("[J]udicial rulings alone almost never constitute a valid basis for a bias or partiality motion."). *See also Johnson v. Warden*, No. 2:16-cv-985, 2020 U.S. Dist. LEXIS 54236, at *49 (S.D. Ohio March 27, 2020) ("Evidence of racial bias cannot be inferred but must be clearly demonstrated in the record."). In short, plaintiff has not presented any basis to reconsider on grounds of bias.

Plaintiff's motion fails to demonstrate any bases for reconsideration under RCFC 59. Thus no response from defendant is necessary, and the motion is denied.[3]

---

[3] Plaintiff also attempted to file a motion for status update regarding his motion for reconsideration. The clerk's office received that document on July 17, 2024, but did not docket it because there is no provision in the court's rules for the filing of such a motion. We allow the motion to be filed and deny it as moot.

4

A012

s/Eric G. Bruggink
ERIC G. BRUGGINK
Senior Judge

5

A013

23-811 C

Case No: _____

IN THE UNITED STATES COURT OF FEDERAL CLAIMS

Larry Golden

Plaintiff, Pro Se

740 Woodruff Rd., #1102

Greenville, South Carolina 29607

atpg-tech@charter.net

(864) 992-7104

LARRY GOLDEN, *Plaintiff,* V. THE UNITED STATES DEFENSE THREAT REDUCTION AGENCY *Defendant.*	**Patent Infringement Pursuant to 28 U.S.C. Section 1498** May 29, 2023

INFORMAL COMPLAINT

1.   Under the Tucker Act, the United States Court of Federal Claims has jurisdiction to adjudicate a claim if the statute, regulation, or constitutional provision that is the basis for that claim "can fairly be interpreted as mandating compensation by the Federal Government for the damage sustained," *United States v. Mitchell*, 463 U.S. 206, 217 (1983), and the plaintiff is "within the class of plaintiffs entitled to recover under the statute if the elements of [the] cause of action are established," *Greenlee County, Arizona v. United States*, 487 F.3d 871, 876 (Fed. Cir.

A014

2007). "There is no further jurisdictional requirement that plaintiff make [] additional nonfrivolous allegation[s] that [he] is entitled to relief under the relevant money-mandating source." *Jan's Helicopter Serv., Inc. v. Federal Aviation Agency.* 525 F.3d 1299, 1307 (Fed. Cir. 2008)."

2.   This is a claim pursuant to 28 U.S.C. § 1498(a) for recovery of Plaintiff's reasonable royalties for the unlicensed use, manufacture for, or by the United States, inventions described in and covered by United States Patent Numbers: 9,096,189; 9,589,439, and 10,163,287. **Exhibits A, B, & C**

JURISDICTION

3.   The jurisdiction of this Court is based on the provisions of 28 U.S.C. § 1498(a).

4.   28 U.S.C. § 1498(a): Whenever an invention described in and covered by a patent of the United States is used or manufactured by or for the United States without license of the owner thereof or lawful right to use or manufacture the same, the owner's remedy shall be by action against the United States in the United States Court of Federal Claims for the recovery of his reasonable and entire compensation for such use and manufacture.

THE PARTIES

5.   Plaintiff Larry Golden is a citizen of South Carolina and has a principal place of business (ATPG Technology, LLC), and residence at 740 Woodruff Road, #1102, Greenville, S.C. 29607.

6.   Defendant, the UNITED STATES DEFENSE THREAT REDUCTION AGENCY (DTRA). The DTRA is both a defense agency and a combat support agency within the U. S. Department of Defense (DoD) for countering weapons of mass destruction and supporting the nuclear enterprise. DTRA provides cross-cutting solutions to enable the DoD, the United States Government, and international partners to deter strategic attack against the United States and its allies; prevent, reduce, and counter WMD and emerging threats; and prevail against WMD-armed adversaries in crisis and conflict. The Solicitation for this initiative is attached as **Exhibit D: DTRA HDTRA-19-S-0005 BAA Call CBI-01**

STANDARD(S) FOR REVIEW

7.   When the United States Court of Appeals for the Federal Circuit in Plaintiff's cases *Golden v. Apple Inc. et al* Case No. 22-1229 and *Golden v. Google* Case No. 22-1267, before filing an opinion on 09/08/2022, the three Circuit Judges of Dyk, Taranto, and Stoll used as their standard of review the following:

> "Under the pleading standards set forth in *Bell Atlantic Corp. v. Twombly*, 550 U.S. 544 (2007), and *Ashcroft v. Iqbal*, 556 U.S. 662 (2009), a court must dismiss a complaint if it fails to allege "enough facts to state a claim to relief that is plausible on its face." *Twombly*, 550 U.S. at 570. This standard "requires more than labels and conclusions, and a formulaic recitation of the elements of a cause of action will not do." *Id.* at 555 (citation omitted). A plaintiff must allege facts that give rise to "more than a sheer possibility that a defendant has acted unlawfully." *Iqbal*, 556 U.S. at 678 (citation omitted). In the patent context, this court has explained that a plaintiff need not "plead facts establishing that each element of an asserted claim is met," *In re Bill of Lading Transmission and Processing Sys. Pat. Litig.*, 681 F.3d 1323, 1335 (Fed. Cir. 2012) (citing *McZeal v. Sprint Nextel Corp.*, 501 F.3d 1354, 1357 (Fed. Cir. 2007)), but must plead "'enough fact[s] to raise a reasonable expectation that discovery will reveal' that the defendant is liable for the misconduct alleged." *Id.* at 1341 (alteration in original) (quoting *Twombly*, 550 U.S. at 556). We review the district court's dismissal of the complaint *de novo. Anand v. Ocwen Loan Servicing, LLC*, 754 F.3d 195, 198 (4th Cir. 2014)."

8.   Upon review, the three Circuit Judges of Dyk, Taranto, and Stoll considered **_all_** of the previous cases directly related to the Apple and Google cases [case nos. 22-1229 and 22-1267] that was currently before the Circuit Court; and, the recommendations, decisions, opinions, and judgements.

9.   The Circuit Judges decided not to dismiss Plaintiff's cases based on the number of times Plaintiff was forced to file because of Court errors [changing the cause of action; improperly petitioning the PTAB; giving the Government another chance at dismissing Plaintiff's case; making a Section 1491(a) the same as a Section 1498(a); CFC adjudicating a 35 U.S.C. Section 271(a) which is outside the Court's jurisdiction; making a violation of antitrust laws the same as 35 U.S.C. Section 271(a); wrongfully dismissing as duplicative; wrongfully

A016

dismissing because of page count, etc.] The *Golden v. Apple* case was dismissed ***without prejudice*** for the following reason:

> "Mr. Golden does not argue that the docketed complaint contains factual allegations beyond those contained in his original complaint or that the allegations in the docketed complaint do anything beyond listing the alleged infringed-upon patent claims and the alleged infringing devices. This is plainly insufficient. We see no error in the district court ***without prejudice*** dismissal of the Apple case."

10.   In *Golden v. Google* CAFC Case No. 22-1267, the case was Vacated and Remanded back to the District Court for the following reason: **Exhibit E**

> "In the Google case, the district court again concluded that Mr. Golden's complaint was frivolous. Here, however, Mr. Golden's complaint includes a detailed claim chart mapping features of an accused product, the Google Pixel 5 Smartphone, to independent claims from U.S. Patent Nos. 10,163,287, 9,589,439, and 9,069,189. The district court discounted this claim chart because it "contains the exact same language as the claim charts previously rejected by the Federal Circuit [in the 2019 case], although Google Pixel 5 Smartphone appears in the far-left column instead of Apple." Dist. Ct. Op. at 4. But to the extent that the chart includes the "exact same language" as previously rejected charts, it is simply the language of the independent claims being mapped to. The key column describing the infringing nature of the accused products is not the same as the complaint held frivolous in the 2019 case. It attempts—whether successfully or not—to map claim limitations to infringing product features, and it does so in a relatively straightforward manner. We conclude that the district court's decision in the Google case is not correct with respect to at least the three claims mapped out in the claim chart. Mr. Golden has made efforts to identify exactly how the accused products meet the limitations of his claims in this chart. On remand, the district court should allow the complaint to be filed and request service of process [] ... We express no opinion as to the adequacy of the complaint or claim chart except that it is not facially frivolous."

11.   The Defendants in both cases asked the three Circuit Judges of Dyk, Taranto, and Stoll to affirm dismissal of Plaintiff's cases because the cases are "frivolous" and that Plaintiff is a "serial filer". The Circuit Judges reviewed the District Court case and decided against it.

12.   What that means is, the Defendant (Government the United States) is collateral estoppel from re-litigating the issue of "frivolousness"; the number of times Plaintiff has file cases; and the cause of actions of those cases, because the issues were actually litigated and conclusively resolved by the three Circuit Judges of Dyk, Taranto, and Stoll in *Golden v. Google* CAFC Case No. 22-1267.

13.   Issue preclusion, or collateral estoppel, precludes a party [Government] from relitigating an issue actually decided in a prior case and necessary to the judgment. In a collateral estoppel case, the issue at the heart of the claim has already been raised and litigated in *Golden v. Google* CAFC Case No. 22-1267.

14.   According to law, any and all defense pleadings of "frivolousness" the Government presents in this case to prejudice Plaintiff, after the *OPINION* filed on 09/08/2022 in *Golden v. Google* Case No. 22-1267, should be disregarded and stricken because of "issue preclusion" and "collateral estoppel".

NATURE OF THE CASE

15.   Plaintiff included in this complaint a claim chart that is practically identical to the Google complaint and claim chart. Stare decisis is the legal doctrine Plaintiff is relying on because it obligates this Court to follow historical cases when making a ruling on a similar case.

16.   Stare decisis ensures Plaintiff that cases with similar scenarios and facts are approached in the same way. Simply put, it binds this Court to follow the legal precedent set by the Federal Circuit in its previous decision in Golden v. *Google* CAFC Case No. 22-1267.

17.   To demonstrate this is not an incidental occurrence Plaintiff provided this Court with a smartphone comparison chart of the Google Pixel 5; Apple iPhone 12; Samsung Galaxy S21; LG V60 ThinQ 5G; & Asus/Qualcomm Smartphone for Snapdragon Insiders. The results are the same, they all have virtually identical elements in their alleged infringing products.

18.   Plaintiff has cured the deficiencies identified in *Golden v. US* CFC Case No. 13-307C. Plaintiff responded to the deficiencies only because this Court allowed the Government to present a defense whereby the sensors had to by "native" to the alleged infringing products. The Federal Circuit disagreed in *Golden v. Google* CAFC Case No. 22-1267 and determine the detection capability can also be CBRN plugins. Third party contractors cannot be held liable for

infringement if performing work for the Government, and with the Government's authorization and consent.

19.   Plaintiff has reproduced a claim chart in this complaint that illustrates sensing mechanisms "native" to the smartphones manufactured by Google, Apple, Samsung, LG, and Qualcomm. The sensing mechanisms include the smartphone cameras, standard sensors, and ports.

20.   To support Plaintiff's claim of products (communication devices) grouped together by common features of design similarities of at least that of a smartphone, a PC, etc. Plaintiff added to the smartphone group a Hewlett Packard PC to demonstrate infringement.

VIOLATION ALLEGED

The United States Department of Defense, "Defense Threat Reduction Agency (DTRA)" has Authorized and Consented to the Infringement of Plaintiff's Patents.

21.   Upon information and belief, the United States Defense Threat Reduction Agency (DTRA), (the United States), beginning in year 2019, with the initiative DTRA HDTRA-19-S-0005 BAA Call CBI-01 has allegedly infringed claim 5 of Plaintiff's '287 patent, claim 23 of Plaintiff's '439 patent, and claim 1 of Plaintiff's '189 patent. Pursuant to the guidelines of 28 U.S.C. § 1498(a): "[w]henever an invention described in and covered by a patent of the United States is used or manufactured by or for the United States without license of the owner thereof or lawful right to use or manufacture the same, the owner's remedy shall be by action against the United States in the United States Court of Federal Claims for the recovery of his reasonable and entire compensation for such use and manufacture", Plaintiff believes the DTRA has "authorized or consented" to the infringement of Plaintiff's '287, '439, and '189 patents.

22.   As a result of implied authorization or consent; the DTRA required the contractors of Draper, Microsoft, Intel, Hewlett Packard, Google, Apple, Samsung, LG, and Qualcomm to integrate "for the Government" its, hazard-awareness-and-response tools into the ATAK, iTAK, and WinTAK for chemical and biological agents and radiological and nuclear threats (CBRN) detection and reporting. Further, the contractors integrated, assembled, modified, or developed CBRN plugins for an end-user device such as Plaintiff's patented smartphones, PCs, and tablets.

AUTHORIZATION OR CONSENT

23.　　The Research & Development Directorate, Chemical and Biological (RD-CB) Department of the Defense Threat Reduction Agency (DTRA) issued on May 7, 2019, a Broad Agency Announcement (BAA) Call CBI-01 "Chemical and Biological Threats: Tactical Assault Kit (TAK) Plugins for Warning & Reporting and Decision Making" under BAA HDTRA1-19-S-0005.

24.　　Under the implied authorization or consent, Draper, Microsoft, Google, Apple, Samsung, LG, Qualcomm, Intel, and Hewlett Packard have "manufactured for the Government" products and devices that allegedly infringes claim 5 of Golden's '287 patent, claim 23 of Golden's '439 patent, and claim 1 of Golden's '189 patent.

25.　　The government's authorization of or consent to a contractor's infringing activity may be express or implied, *TVI Energy Corp. v. Blane*, 806 F.2d 1057, 1060 (Fed. Cir. 1986); *Hughes Aircraft Co. v. United States*, 534 F.2d 889, 901 (Ct. Cl. 1976). To succeed on an implied authorization theory there must be some explicit government action, such as a contracting officer's instruction, or evidence extrinsic to the contract language showing the government's intention to assume liability, *Va. Panel*, 133 F.3d at 870; *Larson*, 26 Cl. Ct. at 370.

26.　　In *Larson v. United States*, the Claims Court recognized that implied authorization "may be found under the following conditions: (1) the government expressly contracted for work to meet certain specifications; (2) the specifications cannot be met without infringing on a patent; and (3) the government had some knowledge of the infringement." *Larson*, 26 Cl. Ct. at 370 (citing *Bereslavsky v. Esso Standard Oil Co.*, 175 F.2d 148, 150 (4th Cir. 1949); *Carrier Corp. v. United States*, 534 F.2d 244, 247–50 (Ct. Cl. 1976); *Hughes*, 534 F.2d at 897–901).

27.　　The purpose behind permitting the government's authorization or consent to be implied is tied to the government's need to procure items without disruption, *TVI Energy*, 806 F.2d at 1060; *Robishaw Eng'g Inc. v. United States*, 891 F. Supp. 1134, 1145 (E.D. Va. 1995) ("[T]he policy purpose behind § 1498 is to insulate the government and its private contractors from 'lawsuits disruptive of the procurement process.'" (quoting H.R. Rep. No. 872, 82d Cong., 1st Sess. 1420 (1951), as it appears in *Northrop Corp. v. McDonnell Douglas Corp.*, 705 F.2d 1030, 1041 (9th Cir. 1983))), and avoid the need for government agencies to perform an exhaustive patent search for products or services they wish to procure.

A020

28.   For example, in *TVI Energy*, the Federal Circuit found implied authorization or consent where the government required a contractor to demonstrate an allegedly infringing device as part of bidding requirements under a United States military solicitation for disposable thermal targets, 806 F.2d at 1060–61. Following the demonstration, one bidder/patent owner, TVI Energy, sued a competing bidder, Blane, for patent infringement. Blane asserted immunity under § 1498(a), despite having no express letter of consent or authorization from the government to infringe any patent. The Federal Circuit nevertheless found implied authorization, stating that "[t]o limit the scope of § 1498 only to instances where the Government requires by specification that a supplier infringe another's patent would defeat the Congressional intent to allow the Government to procure whatever it wished regardless of possible patent infringement."

29.   Courts have often found a contractor, through the government's implied authorization, to be immune from suit from the time it offers to supply or begin to manufacture products for the government, See, e.g., *Robishaw*, 891 F. Supp. at 1141 (citing *Trojan, Inc. v. Shat-R-Shield, Inc.*, 885 F.2d 854, 856–57 (Fed. Cir. 1989); *W.L. Gore & Assocs., Inc. v. Garlock, Inc.*, 842 F.2d 1275, 1282–83 (Fed. Cir. 1988); *TVI Energy*, 806 F.2d at 1059–60; *Stelma, Inc. v. Bridge Elecs*. Co., 287 F.2d 163, 164 (3d Cir. 1961)).

30.   If these two elements—acting "for the government" with its "authorization or consent"—are met, then a contractor who infringes a patent in the course of its performance of work for the government, under any definition of infringement in § 271 of the Patent Act, is shielded from liability. In this respect, § 1498(a) serves as an affirmative defense available to government contractors in patent infringement actions in district court, *Advanced Software Design Corp. v. Fed. Reserve Bank of St. Louis*, 583 F.3d 1371, 1375 (Fed. Cir. 2009); *Toxgon Corp. v. BNFL, Inc.*, 312 F.3d 1379, 1381–82 (Fed. Cir. 2002).

31.   Correlatively, where the government has assumed a contractor's liability, a patent owner can seek judicial relief by filing suit against the government in the USCFC, *IRIS Corp. v. Japan Airlines Corp.*, 769 F.3d 1359, 1363 (Fed. Cir. 2014). However, various government agencies have internal processes to hear administrative claims for patent infringement. Christine Hlavka, Contractor Patent Bandits: Preventing the Government from Avoiding 28 U.S.C. § 1498 Liability for Its Contractors' Unauthorized Use of Patented Material by Outsourcing One or More Steps of the Process Abroad, 37 Pub. Cont. L.J. 321, 324–25 (2008).

A021

32.   Therefore, for Draper, Microsoft, Google, Apple, Samsung, LG, Qualcomm, Intel, and Hewlett Packard "authorization or consent of the Government," does not need to be expressly stated. *See TVI Energy Corp. v. Blane*, 806 F.2d 1057, 1060 (Fed. Cir. 1986) ("[a]uthorizarion or consent by the Government can be express [or] [i]n proper circumstances, Government authorization can be implied."). Indeed, "authorization or consent . . . may be given in many ways other than by . . . direct form of communication--e.g., by contracting officer instructions, [or] by specifications . . . which impliedly sanction and necessitate infringement[.]" *Hughes Aircraft co*, 534 F.2d at 901.

33.   In light of the allegations that the inventions disclosed in patents '287, '439 and '189 were designed to prevent terrorist activity, it is plausible that Draper, Microsoft, Google, Apple, Samsung, LG, Qualcomm, Intel, and Hewlett Packard manufactured infringing devices for the benefit of DTRA to promote national security' see, e.g., *Hughes Aircraft Co.*,534 F.2d at 898 (finding that the government's participation in a satellite program was "for the Government," because the program was vital to the military defense and security of the United States). Moreover, under section 1498(a), "Government authorization or consent" can be implied by circumstances. *See TVI Energy Corp.* 806 F.2d at 1060'

34.   DTRA Government funding of research that led to the development and testing of the accused devices (e.g., CBNE Plugins; applications; chips) supports a reasonable inference that the Government impliedly sanctioned the infringing activity.

35.   A review of the claim charts presented in this Complaint against the Defense Threat Reduction Agency (DTRA) identifies by name; by name and product number; or by name, model and product number, the devices that allegedly infringes Plaintiff's patents.

ANDROID TEAM AWARENESS KIT (ATAK)

36.   Android Team Awareness Kit (ATAK) is an Android smartphone geospatial infrastructure and military situation awareness app. It allows for precision targeting, surrounding land formation intelligence, situational awareness, navigation, and data sharing.

37.   Android is a mobile operating system based on a modified version of the Linux kernel and other open-source software, designed primarily for touchscreen mobile devices such as smartphones and tablets. Android is developed by a consortium of developers known as

A022

the Open Handset Alliance, though its most widely used version is primarily developed by Google. It was unveiled in November 2007, with the first commercial Android device, the HTC Dream, being launched in September 2008.

38.   At its core, the operating system is known as Android Open-Source Project (AOSP) and is free and open-source software (FOSS) primarily licensed under the Apache License. Over 70 percent of smartphones based on Android Open-Source Project run Google's ecosystem (which is known simply as Android)

39.   Android has been the best-selling OS worldwide on smartphones since 2011 and on tablets since 2013. As of May 2021, it had over three billion monthly active users, the largest installed base of any operating system

40.   This Android app is a part of the larger TAK family of products. ATAK has a plugin architecture which allows developers to add functionality. This extensible plugin architecture that allows enhanced capabilities for specific mission sets (Direct Action, Combat Advising, Law Enforcement, Protection Operations, Border Security, Disaster Response, Off-grid Communications, Precision Mapping and Geotagging).

41.   ATAK was initially created in 2010 by the Air Force Research Laboratory, and based on the NASA WorldWind Mobile codebase its development and deployment grew slowly, then rapidly since 2016. The Android Team Awareness Kit or TAK is currently used by thousands of Department of Homeland Security personnel, along with other members of the Homeland Security Enterprise including state and local public safety personnel. It is in various stages of transition across DHS components and is the emerging DHS-wide solution for tactical awareness.

42.   In addition to the Android version, there is also a Microsoft Windows version (WinTAK), an Apple iOS version (iTAK), and finally a Virginia-based military tech firm's (LucyTAK). WinTAK is an application developed for the Microsoft Windows Operating System which uses maps to allow for precise targeting, intelligence on surrounding land formations, navigation, and generalized situational awareness. It was developed in conjunction with to provide similar functionality on a Windows platform.

43.   In January 2015, AFRL began licensing ATAK through TechLink to U.S. companies, for commercial use to support state/local government uses as well as civilian uses. As of January 2020, one hundred companies have licensed ATAK for commercial uses. As of

A023

March 31, 2020, the civilian version of ATAK, referred to as CivTAK has been approved for "Public Release" by Army Night Vision and is available for download on takmaps.com And subsequently named Android Team Awareness Kit (ATAK) - Civilian.

44.   The Defense Threat Reduction Agency (DTRA) has leveraged TAK for enhanced CBRNE situational awareness with the goal of protecting military and civilian populations from intentional or incidental chemical or biological threats and Toxic Industrial Chemicals/Materials (TIC/TIM) hazards.

45.   Under the Broad Agency Announcement from the Joint Science and Technology Office (JSTO) Digital Battlespace Management Division, DTRA funded the development of ATAK, WinTAK, and WebTAK compatible versions of existing decision support tools for chemical and biological warning and reporting, hazard prediction, and consequence assessment.

46.   Through collaboration and innovation, the Defense Threat Reduction Agency has integrated its powerful, hazard-awareness-and-response tools into the Android Tactical Assault Kit (or the Android Team Awareness Kit, ATAK). ATAK is a digital application available to warfighters throughout the DoD. Built on the Android operating system, ATAK offers warfighters geospatial mapping for situational awareness during combat — on an end-user device such as a smartphone or a tablet. Warfighters use ATAK to guide themselves to safety when confronted with a release of chemical and biological agents and radiological and nuclear threats (CBRN).

47.   ATAK can connect to sensors on many platforms (e.g., satellites, drones, smartwatches) and has many plugins that warfighters can download. ATAK provides a single interface for viewing and controlling different CBRN-sensing technologies, whether that is a wearable smartwatch that measures a warfighter's vitals (e.g., heart rate) or a device mounted on a drone to detect chemical warfare agents.

48.   Warfighters positively evaluated the CBRN plug-ins at the 2019 Chemical and Biological Operational Analysis (CBOA) event, where warfighters evaluated several technology prototypes for their utility in chemical and biological defense. Warfighters reported that the CBRN capabilities in ATAK are useful and easy to use with minimal training.

49.   Overall, the U.S. armed forces and their interagency and coalition partners value ATAK and the common operating picture it provides. DTRA continues to develop CBRN-specific plug-in capabilities to support warfighters on the battlefield.

A024

SMARTPHONE COMPARISON BETWEEN THE GOOGLE PIXEL 5; APPLE iPHONE 12; SAMSUNG GALAXY S21; LG V60 ThinQ 5G; & ASUS / QUALCOMM SMARTPHONE FOR SNAPDRAGON INSIDERS

50.   The Federal Circuit on 09/08/2022, in *Larry Golden v. Google LLC*; Case No. 22-1267 — "VACATED AND REMANDED" the relevant Case No: 22-1267 Document 15; back to the District Court "to be filed and request service of process".
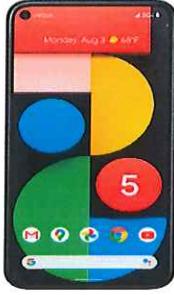
51.   The Federal Circuit determined the complaint, "includes a detailed claim chart mapping features of an accused product, the Google Pixel 5 Smartphone, to independent claims from U.S. Patent Nos. 10,163,287, 9,589,439, and 9,069,189" ... "in a relatively straightforward manner" ... and that the [Circuit] "express no opinion as to the adequacy of the complaint or claim chart except that it is not facially frivolous." **Exhibit E**

Three-Judge Panel: "DISCUSSION. 'Under the pleading standards set forth in *Bell Atlantic Corp. v. Twombly*, 550 U.S. 544 (2007), and *Ashcroft v. Iqbal*, 556 U.S. 662 (2009), a court must dismiss a complaint if it fails to allege "enough facts to state a claim to relief that is plausible on its face." *Twombly*, 550 U.S. at 570 ... [T]his standard "requires more than labels and conclusions, and a formulaic recitation of the elements of a cause of action will not do." *Id.* at 555 (citation omitted). A plaintiff must allege facts that give rise to "more than a sheer possibility that a defendant has acted unlawfully." *Iqbal*, 556 U.S. at 678 (citation omitted) ... this court has explained that a plaintiff ... must plead "'enough fact[s] to raise a reasonable expectation that discovery will reveal' that the defendant is liable for the misconduct alleged."

"Mr. Golden's complaint includes a detailed claim chart mapping features of an accused product, the Google Pixel 5 Smartphone, to independent claims from U.S. Patent Nos. 10,163,287, 9,589,439, and 9,069,189 ... It [claim chart] attempts [] to map claim limitations to infringing product features, and it does so in a relatively straightforward manner ...[W]e conclude that the district court's decision in the Google case is not correct with respect to at least the three claims mapped out in the claim chart. Mr. Golden has made efforts to identify exactly how the accused products meet the limitations of his claims in this chart...."

A025

Claim Chart for the Google Pixel 5 Smartphone (Federal Circuit)

The following Claim Chart is an illustration of literal infringement. At least one of the alleged infringing products of Google (i.e., Google Pixel smartphones 3, 3XL, 3a, 3aXL, 4a, 4a(5G), or 5) is representative of most all the above alleged infringing products of Google asserted in this complaint. At least one of the alleged infringing products of Google (Google Pixel 5) is illustrated to show how the Google Pixel 5 allegedly infringes on at least one of the asserted independent claims of each of the patents-in-suit ('287, '439, and '189 patents).

Google Pixel 5 Smartphone	Patent #: 10,163,287; Independent Claim 5	Patent #: 9,589,439; Independent Claim 23	Patent #: 9,096,189; Independent Claim 1
	A monitoring device, comprising:	A cell phone comprising:	A communication device of at least one of a cell phone, a smart phone, a desktop, a handheld, a PDA, a laptop, or a computer terminal for monitoring products, interconnected to a product for communication therebetween, comprising:
CPU: Octa-core (1 × 2.4 GHz Kryo 475 Prime & 1 × 2.2 GHz Kryo 475 Gold & 6 × 1.8 GHz Kryo 475 Silver) System-on-a-chip: Qualcomm Snapdragon 765G	at least one central processing unit (CPU);	a central processing unit (CPU) for executing and carrying out the instructions of a computer program;	at least one of a central processing unit (CPU) for executing and carrying out the instructions of a computer program, a network processor which is specifically targeted at the networking application domain, or a front-end processor for communication between a host computer and other devices;

A026

Ambient Temperature sensor supported by the Android platform. Measures the ambient room temperature in degrees Celsius (°C). Monitoring air temperatures. Monitoring air temperatures.	at least one temperature sensor in communication with the at least one CPU for monitoring temperature;	X	X
Gravity sensor supported by the Android platform. Measures the force of gravity in m/s2 that is applied to a device on all three physical axes (x, y, z). Motion detection (shake, tilt, etc.).	at least one motion sensor in communication with the at least one CPU;	X	X
Light sensor supported by the Android platform. Measures the ambient light level (illumination) in lx. Controlling screen brightness. Screen: 6-inch flexible OLED display at 432 ppi	at least one viewing screen for monitoring in communication with the at least one CPU;	X	X
Connectivity: Wi-Fi 5 (a/b/g/n/ac) 2.4 + 5.0 GHz, Bluetooth 5.0 + LE, NFC, GPS (GLONASS, Galileo, BeiDou), eSIM capable	at least one global positioning system (GPS) connection in communication with the at least one CPU;	at least one of a satellite connection, Bluetooth connection, WiFi connection, internet connection, radio frequency (RF) connection, cellular connection, broadband connection, long range radio frequency (RF) connection, short range radio frequency (RF) connection, or GPS connection;	at least one satellite connection, Bluetooth connection, WiFi connection, internet connection, radio frequency (RF) connection, cellular connection, broadband connection, long and short-range radio frequency (RF) connection, or GPS connection;

14

A027

Connectivity: Wi-Fi 5 (a/b/g/n/ac) 2.4 + 5.0 GHz, Bluetooth 5.0 + LE, NFC, GPS (GLONASS, Galileo, BeiDou), eSIM capable	at least one of an internet connection or a Wi-Fi connection in communication with the at least one CPU;	wherein at least one of… WiFi connection, internet connection, radio frequency (RF) connection, cellular connection… capable of signal communication with the transmitter or the receiver;	wherein the only type or types of communication with the transmitter and the receiver of the communication device and transceivers of the products is a type or types selected from the group… of satellite, Bluetooth, WiFi…
Connectivity: Wi-Fi 5 (a/b/g/n/ac) 2.4 + 5.0 GHz, Bluetooth 5.0 + LE, NFC, GPS (GLONASS, Galileo, BeiDou), eSIM capable	at least one of a Bluetooth connection, a cellular connection, or a satellite connection in communication with the at least one CPU;	at least one of a… Bluetooth connection, WiFi connection, internet connection… cellular connection… short range radio frequency (RF) connection, or GPS connection;	X
Google's Android operating system features a lock mechanism to secure your phone, known as pattern lock. To set, drag your finger along lines on the screen. To unlock the phone, replicate the pattern drawn. If you fail to solve the pattern too many times, the phone locks and cannot be unlocked without logging into the associated Google account. Google Nest × Yale Lock is connected to the Nest app; you can lock or unlock your door from your phone.	at least one locking mechanism in communication with the at least one CPU for locking the communication device, the at least one locking mechanism configured to at least one of engage (lock) the communication device, disengage (unlock) the communication device, or disable (make unavailable) the communication device;	whereupon the cell phone is interconnected to the cell phone detection device to receive signals or send signals to lock or unlock doors, to activate or deactivate security systems, to activate or deactivate multi-sensor detection systems, or to activate or deactivate the cell phone detection device;	X

15

A028

Pixel phones use USB-C with USB 2.0 power adapters and cables. To charge your phone with a USB-A power adapter, use a USB-C to USB-A cable.	at least one power source comprising at least one of a battery, electrical connection, or wireless connection, to provide power to the communication device;	X	X
BIOMETRICS: Biometric factors allow for secure authentication on the Android platform. The Android framework includes face and fingerprint biometric authentication. Android can be customized to support other forms of biometric authentication (such as Iris).	at least one biometric sensor in communication with the at least once CPU for providing biometric authentication to access the communication device;	wherein the cell phone is equipped with a biometric lock disabler that incorporates at least one of a fingerprint recognition, voice recognition, face recognition, hand geometry, retina scan, iris scan, or signature such that the cell phone is locked by the biometric lock disabler to prevent unauthorized use; and	wherein the communication device is equipped with a biometric lock disabler that incorporates at least one of a fingerprint recognition, voice recognition, face recognition, hand geometry, retina scan, iris scan and signature such that the communication device that is at least one of the cell phone, the smart phone, the desktop, the handheld, the PDA, the laptop or the computer terminal is locked by the biometric lock disabler to prevent unauthorized use
Android Team Awareness Kit, ATAK (built on the Android operating system) provides a single interface for viewing and controlling different CBRN-sensing technologies, whether that is a wearable smartwatch that measures a warfighter's vitals (e.g., heart rate) or a device mounted on a drone to detect chemical warfare agents.	at least one sensor for chemical, biological, or human detection in communication with the at least one CPU;	the cell phone is at least a fixed, portable or mobile communication device interconnected to the cell phone detection device, capable of wired or wireless communication therebetween; and	the communication device is at least a fixed, portable or mobile communication device interconnected to a fixed, portable or mobile product, capable of wired or wireless communication therebetween…

16

A029

Android Team Awareness Kit, ATAK (built on the Android operating system) is a digital application available to warfighters throughout the DoD. ATAK offers warfighters geospatial mapping for situational awareness during combat — on an end-user device such as a smartphone or a tablet. With DTRA's contribution, ATAK now includes chemical, biological, radiological, and nuclear (CBRN) plug-ins.	one or more detectors in communication with the at least one CPU for detecting at least one of chemical, biological, radiological, or explosive agents;	at least one of a chemical sensor, a biological sensor, an explosive sensor, a human sensor, a contraband sensor, or a radiological sensor capable of being disposed within, on, upon or adjacent the cell phone;	wherein the communication device receives a signal via any of one or more products listed in any of the plurality of product grouping categories;
Connectivity: Wi-Fi 5 (a/b/g/n/ac) 2.4 + 5.0 GHz, Bluetooth 5.0 + LE, NFC, GPS (GLONASS, Galileo, BeiDou), eSIM capable	at least one radio-frequency near-field communication (NFC) connection in communication with the at least one CPU…	X	X
Google Nest × Yale Lock is connected to the Nest app; you can lock or unlock your door from your phone. *Android Team Awareness Kit*, ATAK (built on the Android operating system) provides a single interface for viewing and controlling different CBRN-sensing technologies	at least one of a transmitter or a transceiver in communication with the at least one CPU configured to send signals to monitor at least one of a door, a vehicle, or a building, send signals to lock or unlock doors, send signals to control components of a vehicle, send signals to control components of a building, or… detect at least one of a chemical biological… agent such that the communication device is capable of communicating, monitoring, detecting, and controlling.	a transmitter for transmitting signals and messages to a cell phone detection device; a receiver for receiving signals from the cell phone detection device;	a transmitter for transmitting signals and messages to at least one of plurality product groups based on the categories of a multi-sensor detection device, a maritime cargo container, a cell phone detection device, or a locking device; a receiver for receiving signals, data or messages from at least one of plurality product groups based on the categories of a multi-sensor detection device, a maritime cargo container, a cell phone detection device, or a locking device;

17

A030

Google Nest × Yale Lock is connected to the Nest app; you can lock or unlock your door from your phone. *Android Team Awareness Kit*, ATAK (built on the Android operating system) provides a single interface for viewing and controlling different CBRN-sensing technologies	X	X	whereupon the communication device, is interconnected to a product equipped to receive signals from or send signals to lock or unlock doors, activate or deactivate security systems, activate or deactivate multi-sensor detection systems, or to activate or deactivate cell phone detection systems
Android Team Awareness Kit, ATAK (built on the Android operating system) is a digital application available to warfighters throughout the DoD. ATAK offers warfighters geospatial mapping for situational awareness during combat — on an end-user device such as a smartphone or a tablet. With DTRA's contribution, ATAK now includes chemical, biological, radiological, and nuclear (CBRN) plug-ins.	X	a transmitter for transmitting signals and messages to a cell phone detection device; a receiver for receiving signals from the cell phone detection device;	wherein at least one satellite connection, Bluetooth connection, WiFi connection, internet connection, radio frequency (RF) connection, cellular connection, broadband connection… short range radio frequency (RF) connection is capable of signal communication with the transmitter and the receiver of the communication device and transceivers of the products;

A031

Android Team Awareness Kit, ATAK (built on the Android operating system) is a digital application available to warfighters throughout the DoD. ATAK offers warfighters geospatial mapping for situational awareness during combat — on an end-user device such as a smartphone or a tablet. With DTRA's contribution, ATAK now includes chemical, biological, radiological, and nuclear (CBRN) plug-ins.	X	whereupon a signal sent to the receiver of the cell phone detection device from at least one of the chemical sensor, the biological sensor, the explosive sensor, the human sensor, the contraband sensor, or the radiological sensor, causes a signal that includes at least one of location data or sensor data to be sent to the cell phone.	X

I. Central Processing Units (i.e., CPUs, Processors, Chipsets, SoC)

1. Android Platform (i.e., Android Operating System (OS))

a. Application Specific for CBRNE Detection

i. Communication Protocol (i.e., Plug-ins, Bluetooth, Cellular, NFC)

The smartphone has come a long way since the first iPhone launched in 2007. While Apple's iOS is arguably the world's first smartphone operating system, Google's Android is by far the most popular. Android has evolved significantly since first being released on an HTC-made T-Mobile device in 2008.

It wasn't until 2005 that Google purchased Android, Inc., and while there wasn't much info about Android at the time, many took it as a signal that Google would use the platform to enter the phone business. Eventually, Google did enter the smartphone business — but not as a hardware manufacturer. Instead, it marketed Android to other manufacturers, first catching the eye of HTC, which used the platform for the first Android phone, the HTC Dream, in 2008.

List of Features Supported by Google Android Tactical Assault Kit, (ATAK) (or the Android Team Awareness Kit, (ATAK))

- ❖ **BIOMETRICS**: Biometric factors allow for secure authentication on the *Android platform*. The Android framework includes face and fingerprint biometric authentication. Android can be customized to support other forms of biometric authentication (such as Iris).

- ❖ **DISABLING LOCK MECHANISM:** *Google's Android operating system* features a lock mechanism to secure your phone, known as pattern lock. When setting the pattern, you must drag your finger along lines on the screen between different nodes. Afterward, to unlock the phone, you'll need to replicate the pattern drawn. If you fail to solve the pattern too many times, the phone locks and cannot be unlocked without logging into the associated Google account. If you can't log in, you'll have to employ some other methods to restore control of your phone.

- ❖ **CHEMICAL, BIOLOGICAL, RADIOLOGICAL, AND NUCLEAR (CBRN) DETECTION:** Through collaboration and innovation, the Defense Threat Reduction Agency has integrated its powerful, hazard-awareness-and-response tools into the *Android Tactical Assault Kit (or the Android Team Awareness Kit, ATAK)*. ATAK is a digital application available to warfighters throughout the DoD. Built on the *Android operating system*, ATAK offers warfighters geospatial mapping for situational awareness during combat — on an end-user device such as a smartphone or a tablet. With DTRA's contribution, ATAK now includes chemical, biological, radiological, and nuclear (CBRN) plug-ins.

- ❖ **HEART RATE**: *Android Team Awareness Kit, ATAK* provides a single interface for viewing and controlling different CBRN-sensing technologies, whether that is a wearable smartwatch that measures a warfighter's vitals (e.g., heart rate) or a device mounted on a drone to detect chemical warfare agents.

- ❖ **NEAR FIELD COMMUNICATION (NFC)**: Pixel™, Phone by Google - Turn NFC on/off. *Near Field Communication (NFC)* allows the transfer of data between devices that are a few centimeters apart, typically back-to-back. NFC must be turned on for NFC-based apps (e.g., Tap to Pay) to function correctly. NFC is a set of short-range wireless technologies, typically requiring a distance of 4cm or less to initiate a connection. NFC allows you to share small payloads of data between an NFC tag and an Android-powered device, or between two Android-powered devices. Tags can range in complexity.

- ❖ **WARFIGHTERS:** The U.S. armed forces and their interagency and coalition partners value *Android Team Awareness Kit, ATAK* and the common operating picture it provides. DTRA continues to develop *CBRN-specific plug-in capabilities* to support warfighters on the battlefield.

20

A033

The Alleged Infringing Smartphones Google, Apple, Samsung, LG, and Qualcomm that Support either the ATAK or the iTAK

Google Pixel 5 Smartphone	Apple iPhone 12 Smartphone	Samsung Galaxy S21 Smartphone	LG V60 ThinQ 5G	Asus / Qualcomm Smartphone for Snapdragon Insiders
Chipset: Qualcomm Snapdragon 765G **CPU:** Octa-core (1 × 2.4 GHz Kryo 475 Prime & 1 × 2.2 GHz Kryo 475 Gold & 6 × 1.8 GHz Kryo 475 Silver) **OS:** Google Android 11, upgradable to Android 13. **Modem:** Snapdragon® X52 5G Modem-RF System.	**Chipset:** Apple A14 Bionic (5 nm). **CPU:** Hexa-core (2x3.1 GHz Firestorm + 4x1.8 GHz Icestorm). **OS:** iOS 14.1, upgradable to iOS 16.1 **Modem:** Qualcomm's Snapdragon X55 5G modem	**Chipset:** Qualcomm SM8350 Snapdragon 888 5G (5 nm). **CPU:** Octa-core (1x2.84 GHz Cortex-X1 & 3x2.42 GHz Cortex-A78 & 4x1.80 GHz Cortex-A55) - USA/China. **OS:** Google Android 11, upgradable to Android 13 **Modem:** Snapdragon® X60 5G Modem-RF System.	**Chipset:** Qualcomm SM8250 Snapdragon 865 5G (7 nm+). **CPU:** Octa-core (1x2.84 GHz Cortex-A77 & 3x2.42 GHz Cortex-A77 & 4x1.80 GHz Cortex-A55). **OS:** Google Android 10, upgradable to Android 13 **Modem:** Qualcomm's Snapdragon X55 5G modem	**Chipset:** Qualcomm SM8350 Snapdragon 888 5G (5 nm) **CPU:** Octa-core (1x2.84 GHz Cortex-X1 & 3x2.42 GHz Cortex-A78 & 4x1.80 GHz Cortex-A55). **OS:** Google Android 11. **Modem:** Snapdragon® X60 5G Modem-RF System.
Ambient Temperature sensor supported by the Android platform. Measures the ambient room temperature in degrees Celsius (°C). Monitoring air temperatures.	Temperature sensors located within; the sensors monitor the battery and processor's temperature. In extreme temperatures (hot or cold), these sensors shut down the device to prevent damage	Ambient Temperature sensor supported by the Android platform. Measures the ambient room temperature in degrees Celsius (°C). Monitoring air temperatures.	Ambient Temperature sensor supported by the Android platform. Measures the ambient room temperature in degrees Celsius (°C). Monitoring air temperatures.	Ambient Temperature sensor supported by the Android platform. Measures the ambient room temperature in degrees Celsius (°C). Monitoring air temperatures.

21

A034

Gravity sensor supported by the Android platform. Measures the force of gravity in m/s2 that is applied to a device on all three physical axes (x, y, z). Motion detection (shake, tilt, etc.).	Accelerometer (gravity sensor) supported by the iOS platform. Accelerometer/ Motion sensor: This sensor helps the screen automatically switch from landscape to portrait modes and back again based on whether you're holding the phone vertically or horizontally.	Gravity sensor supported by the Android platform. Measures the force of gravity in m/s2 that is applied to a device on all three physical axes (x, y, z). Motion detection (shake, tilt, etc.).	Gravity sensor supported by the Android platform. Measures the force of gravity in m/s2 that is applied to a device on all three physical axes (x, y, z). Motion detection (shake, tilt, etc.).	Gravity sensor supported by the Android platform. Measures the force of gravity in m/s2 that is applied to a device on all three physical axes (x, y, z). Motion detection (shake, tilt, etc.).
Light sensor supported by the Android platform. Measures the ambient light level (illumination) in lx. Controlling screen brightness. Screen: 6-inch flexible OLED display at 432 ppi	Adjusts the screen brightness for current light conditions using the built-in ambient light sensor. Screen: 6.1" Super Retina XDR (OLED). Lock the screen orientation so that it doesn't change when the iPhone is rotated.	Light sensor supported by the Android platform. Measures the ambient light level (illumination) in lx. Controlling screen brightness. Screen: 6.2 inches flexible OLED display at 421 ppi	Light sensor supported by the Android platform. Measures the ambient light level (illumination) in lx. Controlling screen brightness. Screen: 6.8 inches, 109.8 cm2 OLED display at 395 ppi density	Light sensor supported by the Android platform. Measures the ambient light level (illumination) in lx. Controlling screen brightness. Screen: 6.78 inches, 109.5 cm^2 OLED display at 395 ppi density
Connectivity: Wi-Fi 5 (a/b/g/n/ac) 2.4 + 5.0 GHz, Bluetooth 5.0 + LE, NFC, GPS (GLONASS, Galileo, BeiDou), eSIM capable	Connectivity: Wi-Fi 5 802.11 a/b/g/n/ac/6, dual-band, hotspot. Bluetooth 5.0. NFC, GPS, GLONASS, Galileo, QZSS Nano-SIM; eSIM or Dual SIM	Connectivity: Wi-Fi 802.11 a/b/g/n/ac/6, dual-band, Wi-Fi Direct. Bluetooth 5.0, A2DP, LE. NFC, GPS, GLONASS, BDS, GALILEO. Nano-SIM and eSIM or Dual SIM	Connectivity: Wi-Fi 802.11 a/b/g/n/ac/6, dual-band, Wi-Fi Direct, DLNA. Bluetooth 5.1, A2DP, LE, aptX HD. NFC, GPS, GPS, GLONASS, Galileo, BDS. Single SIM (Nano-SIM) or Hybrid Dual SIM (Nano-SIM, dual stand-by)	Connectivity: Wi-Fi 802.11 a/b/g/n/ac/ 6e, dual-band, Wi-Fi Dir. Bluetooth: 5.2, A2DP, LE, aptX HD, aptX Adaptive. NFC, GPS, GLONASS, BDS, Galileo, QZSS, Dual SIM (Nano-SIM, dual stand-by)

22

A035

Connectivity: Wi-Fi 5 (a/b/g/n/ac) 2.4 + 5.0 GHz, Bluetooth 5.0 + LE, NFC, GPS (GLONASS, Galileo, BeiDou), eSIM capable	Connectivity: Wi-Fi 5 802.11 a/b/g/n/ac/6, dual-band, hotspot. Bluetooth 5.0. NFC, GPS, GLONASS, Galileo, QZSS Nano-SIM; eSIM or Dual SIM	Connectivity: Wi-Fi 802.11 a/b/g/n/ac/6, dual-band, Wi-Fi Direct. Bluetooth 5.0, A2DP, LE. NFC, GPS, GLONASS, BDS, GALILEO. Nano-SIM and eSIM or Dual SIM	Connectivity: Wi-Fi 802.11 a/b/g/n/ac/6, dual-band, Wi-Fi Direct, DLNA. Bluetooth 5.1, A2DP, LE, aptX HD. NFC, GPS, GPS, GLONASS, Galileo, BDS. Single SIM (Nano-SIM	Connectivity: Wi-Fi 802.11 a/b/g/n/ac/6e, dual-band, Wi-Fi Dir. Bluetooth: 5.2, A2DP, LE, aptX HD, aptX Adaptive. NFC, GPS, GLONASS, BDS, Galileo, QZSS, Dual SIM (Nano-SIM, dual stand-by)
Connectivity: Wi-Fi 5 (a/b/g/n/ac) 2.4 + 5.0 GHz, Bluetooth 5.0 + LE, NFC, GPS (GLONASS, Galileo, BeiDou), eSIM capable	Connectivity: Wi-Fi 5 802.11 a/b/g/n/ac/6, dual-band, hotspot. Bluetooth 5.0. NFC, GPS, GLONASS, Galileo, QZSS Nano-SIM; eSIM or Dual SIM	Connectivity: Wi-Fi 802.11 a/b/g/n/ac/6, dual-band, Wi-Fi Direct. Bluetooth 5.0, A2DP, LE. NFC, GPS, GLONASS, BDS, GALILEO. Nano-SIM and eSIM or Dual SIM	Connectivity: Wi-Fi 802.11 a/b/g/n/ac/6, dual-band, Wi-Fi Direct, DLNA. Bluetooth 5.1, A2DP, LE, aptX HD. NFC, GPS, GPS, GLONASS, Galileo, BDS. Single SIM (Nano-SIM	Connectivity: Wi-Fi 802.11 a/b/g/n/ac/6e, dual-band, Wi-Fi Dir. Bluetooth: 5.2, A2DP, LE, aptX HD, aptX Adaptive. NFC, GPS, GLONASS, BDS, Galileo, QZSS, Dual SIM (Nano-SIM, dual stand-by)
Google's Android operating system features a lock mechanism to secure your phone, known as pattern lock. To set, drag your finger along lines on the screen. To unlock the phone, replicate the pattern drawn. If you fail to solve the pattern too many times, the phone locks and cannot be unlocked without logging into the associated Google account. Google Nest × Yale Lock is connected to the Nest app; you can lock or unlock your door from your phone.	Apple's iOS operating system features a lock mechanism to secure your phone. After multiple failed attempts to unlock the phone, the phone locks and is disabled (made unavailable). Apple Home Key digital security code is stored in Apple Wallet app. It is based on NFC technology. 2 modes of operation: Express Mode: Bring an iPhone or Apple Watch to the lock. Face ID or Passcode. Must use Face ID / Touch ID or enter a passcode.	Google's Android operating system features a lock mechanism to secure your phone, known as pattern lock. To set, drag your finger along lines on the screen. To unlock the phone, replicate the pattern drawn. If you fail to solve the pattern too many times, the phone locks and cannot be unlocked without logging into the associated Google account. Google Nest × Yale Lock is connected to the Nest app; you can lock or unlock your door from your phone.	Google's Android operating system features a lock mechanism to secure your phone, known as pattern lock. To set, drag your finger along lines on the screen. To unlock the phone, replicate the pattern drawn. If you fail to solve the pattern too many times, the phone locks and cannot be unlocked without logging into the associated Google account. Google Nest × Yale Lock is connected to the Nest app; you can lock or unlock your door from your phone.	Google's Android operating system features a lock mechanism to secure your phone, known as pattern lock. To set, drag your finger along lines on the screen. To unlock the phone, replicate the pattern drawn. If you fail to solve the pattern too many times, the phone locks and cannot be unlocked without logging into the associated Google account. Google Nest × Yale Lock is connected to the Nest app; you can lock or unlock your door from your phone.

23

A036

Pixel phones use USB-C with USB 2.0 power adapters and cables. To charge your phone with a USB-A power adapter, use a USB-C to USB-A cable.	USB-A to Lightning cable or the newer USB-C to Lightning cable with your iPhone. The MagSafe Battery Pack makes on-the-go, wireless charging easy and reliable—just attach it to your iPhone	Samsung USB-C Cable lets you charge your USB-C device as well as sync your data to your smartphone	UrbanX USB-C to USB 3.1 Adapter, USB-C Male to USB-A Female, Uses USB OTG Technology, Compatible with LG V60 ThinQ 5G	ASUS / Qualcomm Smartphone for Snapdragon Insiders Dual Port 32GB USB Type C Memory Stick; 32GB USB Type-C flash drive; Features USB Type-C connector and a traditional USB connector.
BIOMETRICS: Biometric factors allow for secure authentication on the Android platform. The Android framework includes face and fingerprint biometric authentication. Android can be customized to support other forms of biometric authentication (such as Iris).	Apple's iOS operating system allows for Face ID authentication with the iPhone 12. The phone also features a lock mechanism to secure your phone. After multiple failed attempts to unlock the phone, the phone locks and is disabled (made unavailable). Apple Home Key digital security code is stored in Apple Wallet app. It is based on NFC technology. 2 modes of operation: Express Mode: Bring an iPhone or Apple Watch to the lock. Face ID or Passcode. Must use Face ID, Touch ID, or enter a passcode.	BIOMETRICS: Biometric factors allow for secure authentication on the Android platform. The Android framework includes face and fingerprint biometric authentication. Android can be customized to support other forms of biometric authentication (such as Iris).	BIOMETRICS: Biometric factors allow for secure authentication on the Android platform. The Android framework includes face and fingerprint biometric authentication. Android can be customized to support other forms of biometric authentication (such as Iris).	BIOMETRICS: Biometric factors allow for secure authentication on the Android platform. The Android framework includes face and fingerprint biometric authentication. Android can be customized to support other forms of biometric authentication (such as Iris).

24

A037

Android Team Awareness Kit, ATAK (built on the Android operating system) provides a single interface for viewing and controlling different CBRN-sensing technologies, whether that is a wearable smartwatch that measures a warfighter's vitals (e.g., heart rate) or a device mounted on a drone to detect chemical warfare agents.	*iOS Team Awareness Kit,* iTAK (built on the iOS 14.1, or later, operating system) provides an interface for viewing and controlling different CBRN-sensing technologies, whether that is a wearable smartwatch that measures a warfighter's vitals (e.g., heart rate) or a device mounted on a drone to detect chemical warfare agents.	*Android Team Awareness Kit,* ATAK (built on the Android operating system) provides a single interface for viewing and controlling different CBRN-sensing technologies, whether that is a wearable smartwatch that measures a warfighter's vitals (e.g., heart rate) or a device mounted on a drone to detect chemical warfare agents.	*Android Team Awareness Kit,* ATAK (built on the Android operating system) provides a single interface for viewing and controlling different CBRN-sensing technologies, whether that is a wearable smartwatch that measures a warfighter's vitals (e.g., heart rate) or a device mounted on a drone to detect chemical warfare agents.	*Android Team Awareness Kit,* ATAK (built on the Android operating system) provides a single interface for viewing and controlling different CBRN-sensing technologies, whether that is a wearable smartwatch that measures a warfighter's vitals (e.g., heart rate) or a device mounted on a drone to detect chemical warfare agents.
Android Team Awareness Kit, ATAK (built on the Android operating system) is a digital application available to warfighters throughout the DoD. ATAK offers warfighters geospatial mapping for situational awareness during combat — on an end-user device such as a smartphone or a tablet. With DTRA's contribution, ATAK now includes chemical, biological, radiological, and nuclear (CBRN) plug-ins.	*iOS Team Awareness Kit,* iTAK (built on the iOS 14.1, or later, operating system) is a digital application available to warfighters throughout the DHS / DoD. iTAK offers warfighters geospatial mapping for situational awareness during combat — on an end-user device such as a smartphone or a tablet. With DTRA's contribution, iTAK includes chemical, biological, radiological, and nuclear (CBRN) plug-ins.	*Android Team Awareness Kit,* ATAK (built on the Android operating system) is a digital application available to warfighters throughout the DoD. ATAK offers warfighters geospatial mapping for situational awareness during combat — on an end-user device such as a smartphone or a tablet. With DTRA's contribution, ATAK now includes chemical, biological, radiological, and nuclear (CBRN) plug-ins.	*Android Team Awareness Kit,* ATAK (built on the Android operating system) is a digital application available to warfighters throughout the DoD. ATAK offers warfighters geospatial mapping for situational awareness during combat — on an end-user device such as a smartphone or a tablet. With DTRA's contribution, ATAK now includes chemical, biological, radiological, and nuclear (CBRN) plug-ins.	*Android Team Awareness Kit,* ATAK (built on the Android operating system) is a digital application available to warfighters throughout the DoD. ATAK offers warfighters geospatial mapping for situational awareness during combat — on an end-user device such as a smartphone or a tablet. With DTRA's contribution, ATAK now includes chemical, biological, radiological, and nuclear (CBRN) plug-ins.

A038

Connectivity: Wi-Fi 5 (a/b/g/n/ac) 2.4 + 5.0 GHz, Bluetooth 5.0 + LE, NFC, GPS (GLONASS, Galileo, BeiDou), eSIM capable	Connectivity: Wi-Fi 5 802.11 a/b/g/n/ac/6, dual-band, hotspot. Bluetooth 5.0. NFC, GPS, GLONASS, Galileo, QZSS Nano-SIM; eSIM or Dual SIM	Connectivity: Wi-Fi 802.11 a/b/g/n/ac/6, dual-band, Wi-Fi Direct. Bluetooth 5.0, A2DP, LE. NFC, GPS, GLONASS, BDS, GALILEO. Nano-SIM and eSIM or Dual SIM	Connectivity: Wi-Fi 802.11 a/b/g/n/ac/6, dual-band, Wi-Fi Direct, DLNA. Bluetooth 5.1, A2DP, LE, aptX HD. NFC, GPS, GPS, GLONASS, Galileo, BDS. Single SIM (Nano-SIM	Connectivity: Wi-Fi 802.11 a/b/g/n/ac/6e, dual-band, Wi-Fi Dir. Bluetooth: 5.2, A2DP, LE, aptX HD, aptX Adaptive. NFC, GPS, GLONASS, BDS, Galileo, QZSS, Dual SIM (Nano-SIM, dual stand-by)
Google Nest × Yale Lock is connected to the Nest app; you can lock or unlock your door from your phone. *Android Team Awareness Kit*, ATAK (built on the Android operating system) provides a single interface for viewing and controlling different CBRN-sensing technologies	Apple Home Key digital security code is stored in Apple Wallet app. It is based on NFC technology. 2 modes of operation: Express Mode: Bring an iPhone or Apple Watch to the lock. Face ID or Passcode. Must use Face ID / Touch ID, or enter a passcode. *iOS Team Awareness Kit*, iTAK (built on the iOS 14.1, or later, operating system) provides an interface for viewing and controlling different CBRN-sensing technologies	Google Nest × Yale Lock is connected to the Nest app; you can lock or unlock your door from your phone. *Android Team Awareness Kit*, ATAK (built on the Android operating system) provides a single interface for viewing and controlling different CBRN-sensing technologies	Google Nest × Yale Lock is connected to the Nest app; you can lock or unlock your door from your phone. *Android Team Awareness Kit*, ATAK (built on the Android operating system) provides a single interface for viewing and controlling different CBRN-sensing technologies	Google Nest × Yale Lock is connected to the Nest app; you can lock or unlock your door from your phone. *Android Team Awareness Kit*, ATAK (built on the Android operating system) provides a single interface for viewing and controlling different CBRN-sensing technologies

A039

Google Nest × Yale Lock is connected to the Nest app; you can lock or unlock your door from your phone. *Android Team Awareness Kit*, ATAK (built on the Android operating system) provides a single interface for viewing and controlling different CBRN-sensing technologies	Apple Home Key digital security code is stored in Apple Wallet app. It is based on NFC technology. 2 modes of operation: Express Mode: Bring an iPhone or Apple Watch to the lock. Face ID or Passcode. Must use Face ID-Touch ID or enter a passcode. *iOS Team Awareness Kit*, iTAK (built on the iOS 14.1, or later, operating system) provides an interface for viewing and controlling different CBRN-sensing technologies	Google Nest × Yale Lock is connected to the Nest app; you can lock or unlock your door from your phone. *Android Team Awareness Kit*, ATAK (built on the Android operating system) provides a single interface for viewing and controlling different CBRN-sensing technologies	Google Nest × Yale Lock is connected to the Nest app; you can lock or unlock your door from your phone. *Android Team Awareness Kit*, ATAK (built on the Android operating system) provides a single interface for viewing and controlling different CBRN-sensing technologies	Google Nest × Yale Lock is connected to the Nest app; you can lock or unlock your door from your phone. *Android Team Awareness Kit*, ATAK (built on the Android operating system) provides a single interface for viewing and controlling different CBRN-sensing technologies
Android Team Awareness Kit, ATAK (built on the Android operating system) is a digital application available to warfighters throughout the DoD. ATAK offers warfighters geospatial mapping for situational awareness during combat — on an end-user device such as a smartphone or a tablet. With DTRA's contribution, ATAK now includes chemical, biological, radiological, and nuclear (CBRN) plug-ins.	*iOS Team Awareness Kit*, iTAK (built on the iOS 14.1, or later, operating system) is a digital application available to warfighters throughout the DHS / DoD. iTAK offers warfighters geospatial mapping for situational awareness during combat — on an end-user device such as a smartphone or a tablet. With DTRA's contribution, iTAK includes chemical, biological, radiological, and nuclear (CBRN) plug-ins.	*Android Team Awareness Kit*, ATAK (built on the Android operating system) is a digital application available to warfighters throughout the DoD. ATAK offers warfighters geospatial mapping for situational awareness during combat — on an end-user device such as a smartphone or a tablet. With DTRA's contribution, ATAK now includes chemical, biological, radiological, and nuclear (CBRN) plug-ins.	*Android Team Awareness Kit*, ATAK (built on the Android operating system) is a digital application available to warfighters throughout the DoD. ATAK offers warfighters geospatial mapping for situational awareness during combat — on an end-user device such as a smartphone or a tablet. With DTRA's contribution, ATAK now includes chemical, biological, radiological, and nuclear (CBRN) plug-ins.	*Android Team Awareness Kit*, ATAK (built on the Android operating system) is a digital application available to warfighters throughout the DoD. ATAK offers warfighters geospatial mapping for situational awareness during combat — on an end-user device such as a smartphone or a tablet. With DTRA's contribution, ATAK now includes chemical, biological, radiological, and nuclear (CBRN) plug-ins.

27

A040

Android Team Awareness Kit, ATAK (built on the Android operating system) is a digital application available to warfighters throughout the DoD. ATAK offers warfighters geospatial mapping for situational awareness during combat — on an end-user device such as a smartphone or a tablet. With DTRA's contribution, ATAK now includes chemical, biological, radiological, and nuclear (CBRN) plug-ins.	*iOS Team Awareness Kit,* iTAK (built on the iOS 14.1, or later, operating system) is a digital application available to warfighters throughout the DHS / DoD. iTAK offers warfighters geospatial mapping for situational awareness during combat — on an end-user device such as a smartphone or a tablet. With DTRA's contribution, iTAK includes chemical, biological, radiological, and nuclear (CBRN) plug-ins.	*Android Team Awareness Kit,* ATAK (built on the Android operating system) is a digital application available to warfighters throughout the DoD. ATAK offers warfighters geospatial mapping for situational awareness during combat — on an end-user device such as a smartphone or a tablet. With DTRA's contribution, ATAK now includes chemical, biological, radiological, and nuclear (CBRN) plug-ins.	*Android Team Awareness Kit,* ATAK (built on the Android operating system) is a digital application available to warfighters throughout the DoD. ATAK offers warfighters geospatial mapping for situational awareness during combat — on an end-user device such as a smartphone or a tablet. With DTRA's contribution, ATAK now includes chemical, biological, radiological, and nuclear (CBRN) plug-ins.	*Android Team Awareness Kit,* ATAK (built on the Android operating system) is a digital application available to warfighters throughout the DoD. ATAK offers warfighters geospatial mapping for situational awareness during combat — on an end-user device such as a smartphone or a tablet. With DTRA's contribution, ATAK now includes chemical, biological, radiological, and nuclear (CBRN) plug-ins.

Figure 1

Google's "use" of Plaintiff's Patented Central Processing Units (CPUs)

"[T]he Accused Products (i.e., Google, Apple, Samsung, LG, and Asus/Qualcomm smartphones) , which are "computers" (i.e., cell phones, computer tablets, and laptops), include components of a memory, a display, and a *processor*" … "[w]hen in use, the "Find My Device" pre-loaded onto the Accused Product uses a *processor*" … "[t]he "Find My Device" feature displays [] information through a *processor* using data stored in the device's memory" … "[t]he LG Support Page lays out in a step-by-step process how to correctly remotely log in to the *processor* to access [] lock the device" … *See Carolyn Hafeman v. LG Electronics Inc.*

In the above claim chart, the Google, Samsung, LG, and Asus/Qualcomm smartphones have Qualcomm Snapdragon Chipsets; have Octa-core CPUs (*processors*); have Google Android Operating Systems; have Qualcomm Snapdragon Modems; have Google "Find My Device" pre-installed *See Carolyn Hafeman v. LG Electronics Inc.*; have Google Android Team Awareness Kits; have Megapixel cameras for CBR sensing; have cameras for captioning nanopores; Biosensors for CBRNE detection; and, Plug-Ins for CBRN detection.

Figure 2 is a comparative chart of the "megapixel" smartphone cameras used for detecting Chem/Bio agents. For each different way used, it qualifies as an alternative to the ATAK or iTAK.

Google Pixel 5 Smartphone	Apple iPhone 12 Smartphone	Samsung Galaxy S21 Smartphone	LG V60 ThinQ 5G	Asus / Qualcomm Smartphone for Snapdragon Insiders
Google Pixel 5: Dual - 12.2 MP (megapixel), OIS 16 MP (megapixel) Camera lens in cell phone with microfluidic lens functions as camera; uses microscope to focus on a chemical sensor. A *megapixel* camera captures the image from the array of nanopores uses fluid rather than bulky moving parts. The sensors contained in one array is determined by the *pixel* resolution phone camera. *Megapixel* resolution in cell phone cameras; probe a million different spots on the sensor simultaneously. *Tiny sensors tucked into cell phones could map airborne toxins in real time.* Source: https://www.understandingnano.com/cell-phone-sensors-toxins.html	*Apple iPhone 12: Dual - 12 MP (megapixel), OIS 12 MP (megapixel)* Camera lens in cell phone with microfluidic lens functions as camera; uses microscope to focus on a chemical sensor. A *megapixel* camera captures the image from the array of nanopores uses fluid rather than bulky moving parts. The sensors contained in one array is determined by the *pixel* resolution phone camera. *Megapixel* resolution in cell phone cameras; probe a million different spots on the sensor simultaneously. *Tiny sensors tucked into cell phones could map airborne toxins in real time.* Source: https://www.understandingnano.com/cell-phone-sensors-toxins.html	*Samsung Galaxy S21: Triple - 12 MP (megapixel), OIS 64 MP (megapixel)* Camera lens in cell phone with microfluidic lens functions as camera; uses microscope to focus on a chemical sensor. A *megapixel* camera captures the image from the array of nanopores uses fluid rather than bulky moving parts. The sensors contained in one array is determined by the *pixel* resolution phone camera. *Megapixel* resolution in cell phone cameras; probe a million different spots on the sensor simultaneously. *Tiny sensors tucked into cell phones could map airborne toxins in real time.* Source: https://www.understandingnano.com/cell-phone-sensors-toxins.html	*LG V60 ThinQ 5G: Dual - 64 MP (megapixel), OIS 13 MP (megapixel)* Camera lens in cell phone with microfluidic lens functions as camera; uses microscope to focus on a chemical sensor. A *megapixel* camera captures the image from the array of nanopores uses fluid rather than bulky moving parts. The sensors contained in one array is determined by the *pixel* resolution phone camera. *Megapixel* resolution in cell phone cameras; probe a million different spots on the sensor simultaneously. *Tiny sensors tucked into cell phones could map airborne toxins in real time.* Source: https://www.understandingnano.com/cell-phone-sensors-toxins.html	*Asus / Qualcomm: Triple - 64 MP (megapixel) OIS; 8 MP, 12MP (mega)* Camera lens in cell phone with microfluidic lens functions as camera; uses microscope to focus on a chemical sensor. A *megapixel* camera captures the image from the array of nanopores uses fluid rather than bulky moving parts. The sensors contained in one array is determined by the *pixel* resolution phone camera. *Megapixel* resolution in cell phone cameras; probe a million different spots on the sensor simultaneously. *Tiny sensors tucked into cell phones could map airborne toxins in real time.* Source: https://www.understandingnano.com/cell-phone-sensors-toxins.html

Figure 2

A042

Figure 3 is a visual display of different ways the smartphone camera [1][2] can be used for detecting Chem/Bio agents. For each different way used, it qualifies as an alternative to the ATAK or iTAK.

Figure 3

---

1 The camera captures the image from the array of nanopores that uses fluid rather than bulky moving parts. The sensors contained in one array is determined by the resolution phone camera. The resolution in cell phone cameras; probe a million different spots on the sensor simultaneously. *Tiny sensors tucked into cell phones could map airborne toxins in real time.* Source: https:// www.understanding nano.com/cell-phone-sensors-toxins.html

2 Hyperspectral imaging scans for light frequencies that humans can't see in order to identify the unique chemical signatures of different substances. They say their device, which can be mass produced, is compatible with all standard smartphone cameras. *These New Smartphone Cameras Could Tell You What an Object Is Made of* https://www.sciencealert.com/new-smartphone-cameras-could-tell-you-what-an-object-is-made-of

A043

Figure 4 describes how at least nine (9) standard sensors for the Google, Apple, Samsung, LG, and Asus/Qualcomm smartphones can be used as "biosensors". Each Biosensor qualifies as an alternative to ATAK or iTAK.
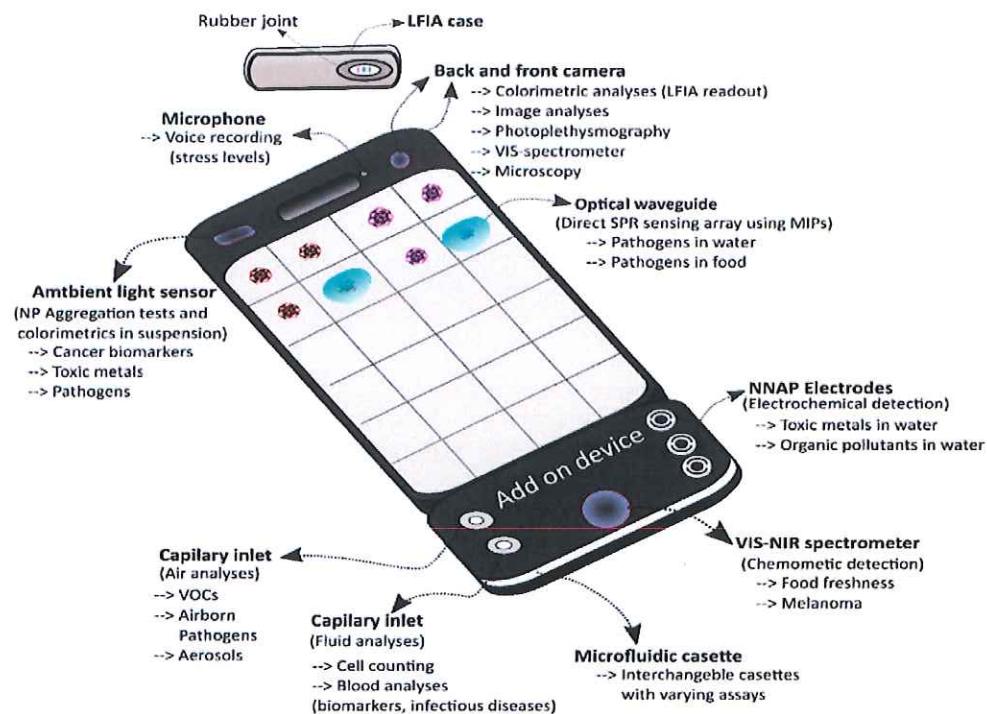

Figure 4

The Smartphones Biosensors:

1. Ambient light sensor: Cancer biomarkers; Toxic metals; Pathogens
2. Capillary inlet: (Air analysis). Airborne Pathogens; Aerosols
3. Capillary inlet: (Fluid analysis). Blood analysis; Biomarkers
4. Microfluidic cassette: Interchangeable cassettes with varying assays
5. VIS-NIR spectrometer: Food freshness; Melanoma
6. NNAP Electrodes: Toxic metals and Organic pollutants in water
7. Optical Waveguide: Pathogens in water and food
8. Back and front camera: Colorimetric analysis; Image analysis
9. Microphone: Voice recording stress levels

31

A044

Figure 5 list some of the same standard sensors illustrated in Figure 4. The port on smartphones is used for the CBRN *plug-ins* included in ATAK or iTAK.
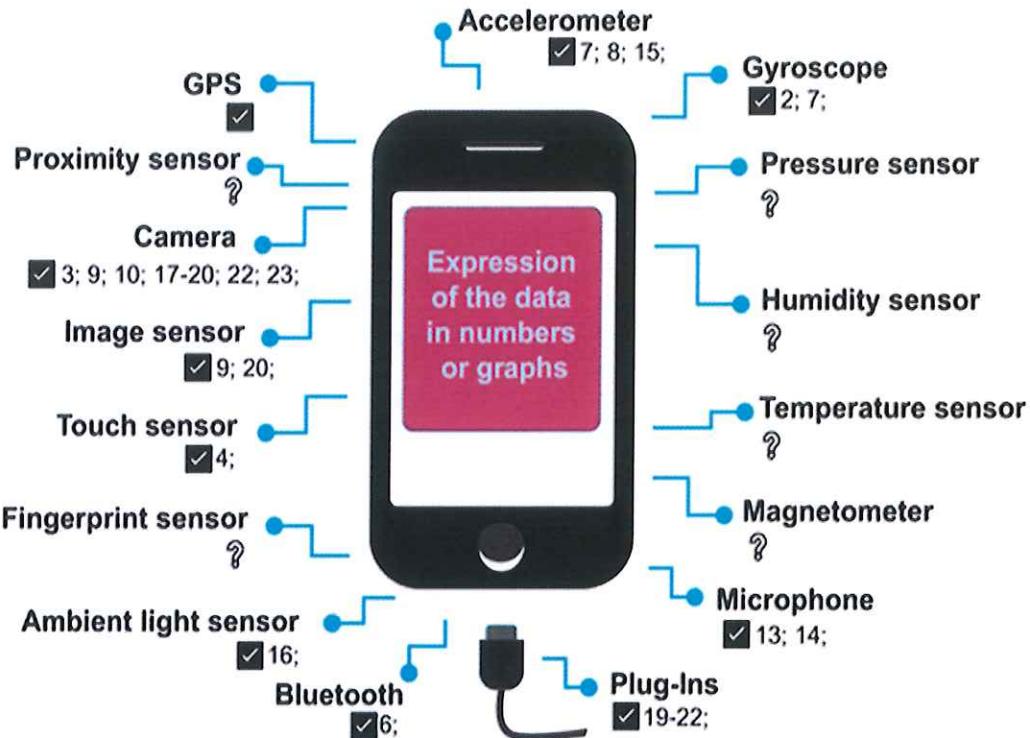

Figure 5

ATAK and iTAK are digital applications available to warfighters throughout the DoD. Built on the Android operating system and iOS operating systems, ATAK and iTAK offers warfighters geospatial mapping for situational awareness during combat — on an end-user device such as a smartphone or a tablet. With DTRA's contribution, ATAK and iTAK now includes chemical, biological, radiological, and nuclear (CBRN) *plug-ins*.

Just having a plug-in is not all that's involved. There has to be an app specific software to sync the chemical, biological, radiological, and nuclear sensors to the smartphone plus the Google Android Operating System.

A045

MICROSOFT WINDOWS (WINTAK)

52.   In addition to the Android version (ATAK) CBRN plug-ins for smartphones, there is also a Microsoft Windows version (WinTAK). WinTAK is an application developed for the Microsoft Windows Operating System which uses maps to allow for precise targeting, intelligence on surrounding land formations, navigation, and generalized situational awareness. It was developed in conjunction with ATAK to provide similar functionality on a Windows platform.

53.   The Defense Innovation Marketplace is your centralized source for Department of Defense (DoD) science and technology (S&T) planning, acquisition resources, funding and financial information. Under the Broad Agency Announcement from the Joint Science and Technology Office (JSTO) Digital Battlespace Management Division, DTRA funded the development of ATAK, WinTAK, and WebTAK compatible versions of existing decision support tools for chemical and biological warning and reporting, hazard prediction, and consequence assessment.

54.   ATAK is an Android®-based GIS moving map application. WinTAK is Microsoft Windows®-based. ATAK was developed to provide SpyGlass-like C2, Situational Awareness and planning capabilities on smartphones and tablets. WinTAK was developed to provide a Windows-based application with a user interface similar to ATAK.

55.   ATAK/WinTAK provides ground users and pilots a meaningful, geospatial site picture and inter-operates with other situational awareness tools including SpyGlass, RaptorX, FalconView, and other legacy systems. Both support most of the standardized image/map formats. Its standalone capabilities include moving map functions independent of cellular/Wi-Fi network. Additionally, these mobile applications allow maps to be loaded during mission pre-planning or execution phase. It utilizes internal and external GPS sources

56.   ATAK/WinTAK variations are currently utilized by many branches of federal, state, and local governments and partner nations.

57.   Draper, one of the nation's leading technology developers for national security, will build on its support for the warfighter under a new contract to operate and maintain the Tactical Assault Kit, or TAK, a widely used communications system for the military. The company recently received a sole-source contract with the Defense Threat Reduction Agency (DTRA) of the U.S. Department of Defense.

A046

58.   The $415,000 contract calls for Draper to provide maintenance support, technical services, testing, evaluation and training for TAK. The TAK application supports the Nuclear Enterprise Contingency Operations Department's (NE-COs) various chemical, biological, radiological and nuclear (CBRN) detector systems.

59.   Draper has developed software for every version of TAK since it was first developed by the Department of Defense. The software is available as ATAK for Android devices, WinTAK for Windows and WebTAK for the web. The company's long experience with the application and with warfighter systems overall were major reasons Draper will expand its role from research and development to operation and maintenance of the TAK platform, according to Brian Alligood, Draper's program manager for TAK. https://www.draper.com/news-releases/draper-tapped-us-department-defense-provide-services-and-support-tactical-assault-kit

60.   Tactical Assault Kit (TAK) is a situational awareness solution designed for military and first responder personnel. On the original development team for ATAK for Android devices under the U.S. Air Force Research Laboratory, Draper contributed to initial design and core software. Draper also worked on WinTAK for Windows, and it developed WebTAK as a browser-based capability.

61.   Draper designed a chemical, biological, radiological and nuclear (CBRN) Plugin to enable users to integrate CBRN sensors into TAK, collect CBRN sensor data, display it on a map and livestream it across the TAK network to other users. CBRN plugins for ATAK, WinTAK and WebTAK are operational in the field.

62.   Below, is an illustrative claim chart of how the HP ZBook PC directly infringes claim 5 of Golden's '287 patent, and claim 1 of Golden's '189 patent.

63.   To satisfy the limitation for CBRN that is internal the HP ZBook PC is Intel's Loihi Neuromorphic Chip to Learn and Recognize the Scents of 10 Hazardous Chemicals. Intel Labs' Nabil Imam holds a Loihi neuro-morphic chip in his Santa Clara, California, neuro-morphic computing lab. (Walden Kirsch/Intel Corp)

64.   To satisfy the limitation for CBRN that is external the HP ZBook PC is WinTAK. WinTAK was developed to provide a Windows-based application. Draper designed a chemical, biological, radiological and nuclear (CBRN) Plugin to enable users to integrate CBRN sensors into WinTAK.